WHAT IS CLAIMED IS:

1. A method of forming a secure peer-to-peer group, comprising the steps of:

generating a group public/private key pair;

generating a group identification as a hash of the group public key; and

defining group security properties.

2. The method of claim 1, further comprising the steps of:

obtaining a public key of a peer;

forming a group membership certificate containing the peer's public key and signed with the group private key; and

sending the group membership certificate to the peer to invite the peer to join the group.

3. The method of claim 1, further comprising the step of generating a group shared key to be used to encrypt group traffic.

4. The method of claim 2, wherein the step of forming a group membership certificate comprises the step of forming a group membership certificate having a structure [Version, ID, Peer ID, Serial Number, Validity, Algorithms, P_{ID}, P_{Issuer}]K_{Issuer}.

5. The method of claim 2, further comprising the steps of:

receiving a connect message from the peer containing the group certificate signed by a private key pair of the peer's public key;

authenticating the group certificate signed by the peer's private key; and

when the step of authenticating is successful,

sending an accept message to the peer, and

sending the group shared key to the peer.

6. The method of claim 5, wherein the step of authenticating comprises the steps of:

verifying that a signature of the certificate is valid;

verifying that the certificate has not expired;

verifying that the hash of the peer's public key matches the peer identification;

opportunistically verifying ownership of the certificate.

7. The method of claim 5, wherein the step of authenticating comprises the steps of:

determining if the certificate is listed in a group certificate revocation list (GCRL);

determining if any certificates in a chain of group membership certificates is listed in the GCRL;

when any certificates in the chain is listed in the GCRL, determining if a date of revocation of the certificate in the chain is before a date of issue of the peer's certificate; and

when the date of revocation is after the date of issuance, issuing a new group certificate to the peer.

8. In a secure peer-to-peer group having a predefined public/private key pair (P_G/K_G), a method of inviting a peer to join the group, comprising the steps of:

obtaining a public key (P_{U1}) of a peer;

forming a first group membership certificate containing the peer's public key (P_{U1}) and a second membership certificate signed with the group private key (K_G), the first group membership certificate being signed with a private key of an issuer (K_{U2}); and

sending the group membership certificate to the peer to invite the peer to join the group.

9. The method of claim 8, wherein the step of forming a group membership certificate comprises the step of forming a group membership certificate having a structure $((P_{U1})K_G)K_{U2})$.

10. The method of claim 8, further comprising the steps of:

receiving a connect message from the peer containing a third group certificate comprising the first group certificate signed by a private key pair of the peer's public key;

authenticating the group certificate signed by the peer's private key; and

when the step of authenticating is successful,

sending an accept message to the peer, and

sending a group shared key to the peer.

11. The method of claim 10, wherein the step of authenticating comprises the steps of:

verifying that a signature of the third certificate is valid;

verifying that the third certificate has not expired;

verifying that the hash of the peer's public key matches a peer identification;

opportunistically verifying ownership of the third certificate.

12. The method of claim 10, wherein the step of authenticating comprises the steps of:

determining if the third certificate is listed in a group certificate revocation list (GCRL);

determining if either of the first and second certificates is listed in the GCRL;

when either of the first and second certificates is listed in the GCRL, determining if a date of revocation is before a date of issuance of the third certificate; and

when the date of revocation is after the date of issuance, issuing a new group certificate to the peer.

13. A method of securely joining a peer-to-peer group by a peer having a public and a private key, comprising the steps of:

receiving a group invitation containing an invitation certificate having a group ID provided therein;

resolving the group ID to find a member of the group;

sending a connect message to the member containing the invitation certificate signed with the private key;

receiving an accept message from the member containing a group membership certificate signed by a private key of the member; and

receiving a group shared key to enable decryption of group traffic.

14. The method of claim 13, further comprising the step of authenticating the group membership certificate signed by the private key of the member to ensure the member's association with the group.

15. The method of claim 14, further comprising the step of resolving the group ID to find a second member of the group to which to connect when the step of authenticating the group membership certificate signed by the private key of the member fails.

16. The method of claim 14, wherein the step of authenticating comprises the steps of:

verifying that a signature of the group membership certificate is valid;

verifying that the group membership certificate has not expired;

verifying that the hash of the member's public key matches a member identification;

opportunistically verifying ownership of the group membership certificate.

17. The method of claim 13, wherein the step of receiving a group invitation containing an invitation certificate having a group ID provided therein comprises the step of receiving a group invitation from a first member containing an invitation certificate and a group membership certificate; and

wherein the step of resolving the group ID to find a member of the group comprises the step of resolving the group ID to find a second member of the group; and

wherein the step of sending a connect message to the member containing the invitation certificate signed with the private key comprises the step of sending a connect message to the second member containing the invitation certificate and the group membership certificate from the first member.

18. A method of securely admitting a peer to a peer-to-peer group, comprising the steps of:

receiving a connect message from the peer containing an invitation certificate signed by a private key of the peer;

authenticating the invitation certificate signed by the peer's private key; and

when the step of authenticating is successful,

sending an accept message to the peer, and

sending a group shared key to the peer.

19. The method of claim 18, wherein the step of authenticating comprises the steps of:

verifying that a signature of the invitation certificate is valid;

verifying that the invitation certificate has not expired;

verifying that a hash of the peer's public key matches a peer identification.

20. The method of claim 18, wherein the step of receiving a connect message from the peer containing an invitation certificate signed by a private key of the peer comprises the step of receiving a connect message from the peer containing an invitation certificate and a group membership certificate from a member of the group that issued the invitation certificate.

21. The method of claim 20, wherein the step of authenticating comprises the steps of:

determining if the group membership certificate is listed in a group certificate revocation list (GCRL);

when the group membership certificate is listed in the GCRL, determining if a date of revocation is before a date of issuance of the invitation certificate; and

when the date of revocation is after the date of issuance, issuing a new group certificate to the peer.

22. A computer-readable medium having computer-executable instructions for performing the steps of claim 1.

23. A computer-readable medium having computer-executable instructions for performing the steps of claim 8.

24. A computer-readable medium having computer-executable instructions for performing the steps of claim 13.

25. A computer-readable medium having computer-executable instructions for performing the steps of claim 18.